Office of the Governor
State Chief Information Officer

SECURITY

Chapter 11 – Delivering Training and Staff Awareness

Scope: These standards apply to all public agencies, their agents or designees subject to N.C.G.S. Article 3D of Chapter 147, "State Information Technology Services."

Statutory Authority: N.C.G.S. 147-33.110

Section 01 Awareness

110101 Delivering Awareness Programs to Permanent Staff

Purpose: To provide awareness programs that ensure employees are familiar with information technology security policies, standards and procedures.

STANDARD

The senior management of each agency shall lead by example by ensuring that information security is given a high priority in all current and future activities and initiatives. The agency, through senior management, shall provide regular and relevant information security awareness communications to all staff by various means, which include but are not limited to the following:

- Electronic updates, briefings, pamphlets and newsletters.
- Information security awareness tools to enhance awareness and educate staff on information technology security threats and the appropriate safeguards.
- An employee handbook or summary of information security policies, which shall be formally delivered to and signed by employees before they access agency resources.

ISO 17799: 2005 REFERENCE
8.2.2 Information security awareness, education and training

110102 Third Party Contractor: Awareness Programs

Purpose: To ensure that contractors are familiar with information technology security policies, standards and procedures.

STANDARD

All contractors shall have provisions in their contracts with State agencies that set forth the requirement that they must comply with all agency information technology security policies. The agency shall provide contractors with regular and relevant information technology security policies. The agency shall provide regular and relevant information security awareness communications to contractors by various means, which include but are not limited to the following:

- An handbook or summary of information security policies, which shall be formally delivered to and signed by contractors before they begin work.
- Mandatory information security awareness training before beginning work.
- Formal information technology security training appropriate for work responsibilities, on a regular basis and whenever their work responsibilities change
- Training in information security threats and safeguards, with the extent of technical details to reflect the contractor's individual responsibility for configuring and maintaining information security.

ISO 17799: 2005 REFERENCES
6.2.3 Addressing security in third party agreements
8.2.2 Information security awareness, education and training

110103 Delivering Awareness Programs to Temporary Staff

The standard recommended for this section is covered by Standard 110101

110104 Drafting Top Management Security Communications to Staff

Purpose: To ensure that top management takes the lead in giving information security a high priority throughout the agency.

STANDARD

Senior management within the agency shall ensure that information security communications are given priority by staff and shall support information security education programs.

ISO 17799: 2005 REFERENCE
5.1.2 Review of the information security policy

110105 Providing Regular Information Updates to Staff

Purpose: To ensure regular and relevant information is passed down to staff from senior management.

STANDARD

Senior management shall continually provide information relevant to effective information security practices to staff members.

On a periodic basis, senior management shall receive input from information security staff on the effectiveness of the organization's information security measures and recommended improvements.

ISO 17799: 2005 REFERENCE
5.1.2 Review of the information security policy

Section 02 Training

110201 Information Security Training on New Systems

Purpose: To ensure that employees, contractors and temporary employees understand the security implications of new technology.

STANDARD

All users of new systems shall receive training to ensure that their use of the systems is effective and does not compromise information security. Agencies shall train users on how new systems will integrate into their current responsibilities. Agencies shall notify staff of all existing and any new policies that apply to new systems.

ISO 17799: 2005 REFERENCE
8.2.2 Information security awareness, education and training

110202 Information Security Officer: Training

Purpose: To ensure that the agency information security officer receives adequate training.

STANDARD

The information security officer of each agency or his/her equivalent, at a minimum, shall receive annual formalized training on the latest threats to information technology systems and on information security protocols. Senior management shall work with the information security officer on a regular basis to provide the information security officer with knowledge of the agency's operational and strategic objectives.

The training for the information security officer must include new technologies to combat threats and updates on new threats to network security and may include updated incident response protocols.

GUIDELINES

Training may be enhanced through:

- Membership in technical societies, clubs, boards, or focus groups.
- Subscriptions to technical documents such as newsletters, magazines and white papers.

- Self-study and certifications relevant to information security.

ISO 17799: 2005 REFERENCE
8.2.2 Information security awareness, education and training

110203 User: Information Security Training

Purpose: To ensure that all users receive adequate training.

STANDARD

All agencies shall provide training to users on relevant information security threats and safeguards. The extent of technical training shall reflect the employee's or contractor's individual responsibility for configuration and/or maintaining information security systems. When staff members change jobs, their information security needs must be reassessed, and any new training on procedures or proper use of information-processing facilities shall be provided as a priority.

Agency training shall include but not be limited to the following:

- Mandatory information security awareness training before beginning work.
- Formal information technology security training appropriate for work responsibilities, on an annual basis.
- Training in information security threats and safeguards, with the technical details to reflect the employee's or contractor's individual responsibility for configuring and maintaining information security.

ISO 17799: 2005 REFERENCE
8.2.2 Information security awareness, education and training

110204 Technical Staff: Information Security Training

Purpose: To ensure that agency technical staff receive adequate training.

STANDARD

Agencies shall make specialized training available for technical staff in critical areas of information technology security, including vendor specifically recommended safeguards to improve:

- Server and PC security management.
- Packet-filtering techniques implemented on routers, firewalls, etc.
- Intrusion detection and prevention.
- Software configuration, change and patch management.
- Virus prevention/protection procedures.
- Business continuity practices and procedures.

When staff members who are responsible for information technology systems change jobs, their information security needs must be reassessed, and any new training on procedures or proper use of information-processing facilities shall be provided as a priority.

ISO 17799: 2005 REFERENCE
8.2.2 Information security awareness, education and training

110205 Training New Recruits in Information Security

Purpose: To ensure that new employees are aware of good information security practices.

STANDARD

All agencies shall provide new employees and contractors with mandatory information security training as part of job orientation.

ISO 17799: 2005 REFERENCE
8.2.2 Information security awareness, education and training

HISTORY

Approved by State CIO: November 18, 2005
Original Issue Date: November 18, 2005
Subsequent History:

Standard Number	Version	Date	Change/Description

Old Security Policy/Standard	New Standard Numbers
Chapter 11 is comprised of new standards not covered under earlier policies or standards.	